青警本情第６６号
平成２３年３月２８日

各　所　属　長　殿

青森県警察本部長

青森県警察情報セキュリティ対策基準の制定について

このたび、青森県警察情報セキュリティ対策基準を別添のとおり制定し、平成２３年５月１日から実施することとしたが､制定の趣旨及び要点は次のとおりであるから、所属職員に周知徹底し、事務処理上誤りのないようにされたい。

なお、「青森県警察情報セキュリティ対策基準の制定について」（平成２２年３月３０日付け青警本情第７１号。以下「旧対策基準」という。）は廃止する。

記

１　制定の趣旨

本県警察における警察情報システムの情報セキュリティの維持に関し必要な事項については、旧対策基準により実施してきたところであるが、警察庁の「警察情報セキュリティ対策基準」が改正されたことから、管理体制、情報の分類を改正するなど所要の整備を行ったものである。

２　制定に伴う改正要点

本対策基準の制定に伴う主な改正点は、次のとおりである。

(1)　用語の定義（第１関係）

「入出力資料」、「ドキュメント」の定義を修正し、「外部記録媒体」、「外部回線」の定義を追加した。

(2)　管理体制（第２関係）

ア　システムセキュリティ責任者

警察情報システムについて必要なセキュリティ要件を備えるため、当該システムの計画段階からシステムセキュリティ責任者を設置し、システム整備を担当する所属の長とした。

イ　システムセキュリティ維持管理者

旧対策基準の「システムセキュリティ管理者」を「システムセキュリティ維持管理者」に名称変更し、電子計算機等の管理者権限を保有する所属の長とした。

(3) 情報の分類（第３関係）

情報の分類の表記をⅠ・Ⅱ・Ⅲの数値表記から、高・中・低の漢字表記に改めるとともに、「完全性」及び「可用性」を高・低の２分類とした。

別添

青森県警察情報セキュリティ対策基準

第１　総則

１　目的

この対策基準は、青森県警察情報セキュリティ要綱（平成２２年３月３０日付け青警本情第６８号。以下「要綱」という。）第５の２の規定に基づき、警察情報システムの情報セキュリティの維持に関し必要な事項を定めるものとする。

２　用語の定義

この対策基準において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 警察情報セキュリティポリシー

要綱及び要綱に基づいて定められた情報セキュリティに関する事項をいう。

(2) 入出力資料

警察情報システムに入力された又は警察情報システムにより出力された情報を記録した文書、図画及び電磁的記録（作成中のものを含む。）をいう。

(3) ドキュメント

警察情報システムに関する以下に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。

ア　システムドキュメント

(ｱ) システム仕様書

(ｲ) システム設計書（情報の処理の手順並びに機器及びプログラムの構成の概要の記録をいう。）

(ｳ) プログラム仕様書（情報の処理の手順の概要の記録をいう。）

(ｴ) プログラムリスト

(ｵ) 操作指示書（システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）

イ　取扱説明書

システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。

(4) 外部記録媒体

フロッピーディスク、フラッシュメモリ、ＤＶＤ規格媒体等警察情報システムに接続し情報を入出力する電磁的記録媒体をいう。

(5) 情報

入出力資料、ドキュメント又は外部記録媒体若しくは警察情報システム内部に記録された情報をいう。

(6) アクセス

警察情報システムにデータを入力し、又は警察情報システムからデータを出力することをいう。

(7) アクセス権者

アクセスを行う権限を与えられた者をいう。

(8) アクセス範囲

アクセス権者ごとにその者が行うことができるアクセスの範囲をいう。

(9) ユーザＩＤ

アクセス権者を識別するためにアクセス権者ごとに一意に付与された文字列をいう。

(10) パスワード

警察情報システムを利用しようとする者がアクセス権者本人であるかどうかを検証するため用いられる文字列をいう。

(11) 認証

ユーザＩＤ、パスワード等を警察情報システムに入力することなどにより、アクセス権者が正当な者であるか否かを検証することをいう。

(12) データベース装置

警察情報システムを構成するメインフレーム、サーバ等の電子計算機及びこれらに附置されるシステム管理を行う電子計算機をいう。

(13) ネットワーク機器

警察情報システムを構成するルータ、レイヤ３スイッチ、スイッチングハブ等の機器若しくは伝送通信装置又はこれらから出力されるデータを利用することによりネットワークを管理する機能を有する機器をいう。

(14) 持ち出し用ＰＣ

警察情報システムのうち、同一の警察の庁舎内から移動して運用するものをいう。

(15) 外部回線

警察機関の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電子通信回線をいう。

第２　管理体制

１　システムセキュリティ責任者

(1) 警察情報システムの整備を担当する所属にシステムセキュリティ責任者を置き、それぞれ当該所属長をもって充てる。

(2) システムセキュリティ責任者は、整備する警察情報システムに関し、２の(2)及び３の(2)の事務を処理するに当たって必要なセキュリティ要件を当該警察情報システムが備えるための事務を処理する。

２　システムセキュリティ維持管理者

(1) 警察情報システムを構成する電子計算機及びネットワーク機器の管理者権限

を保有する所属に、システムセキュリティ維持管理者を置き、それぞれ当該所属長をもって充てる。

(2) システムセキュリティ維持管理者は、担当する警察情報システムの維持管理時における情報セキュリティに係る事務を処理する。

3　運用管理者

(1) 所属に運用管理者を置き、所属長をもって充てる。

(2) 運用管理者は、所属における警察情報システムの運用に関し、情報セキュリティの維持その他の警察情報システムによる処理に係る情報の適正な取扱いを確保するために必要な事務を処理する。

4　運用管理補助者

(1) 所属に運用管理補助者を置き、次長等をもって充てる。

(2) 運用管理補助者は、運用管理者の事務を補佐するものとする。

(3) 分庁舎担当副署長等

警察署の分庁舎担当副署長等は、運用管理補助者と連携して、運用管理者の事務を補佐するものとする。

5　取扱責任者

(1) 所属に取扱責任者を置き、次に掲げる者をもって充てる。

ア　本部所属にあっては、運用管理者が所属職員の中から指定する課長補佐等（方面隊長、分駐隊長及び警部相当一般職員を含む。）

イ　警察署にあっては、各課長（次長が課長を兼務している場合は、運用管理者が指定する係長等）

(2) 取扱責任者は、警察情報システムの運用及び当該機器に係る情報の適正な取扱いについて、運用管理者及び運用管理補助者の指示により、次に掲げる事務を処理するものとする。

ア　警察情報システムを構成する機器及び外部記録媒体の保管管理、点検及び持ち出し等に関すること。

イ　その他運用管理者が必要と認めること。

6　副取扱責任者

(1) 運用管理者は、取扱責任者を補助するため、次に掲げる者を副取扱責任者として指定することができるものとする。

ア　本部所属及び警察署にあっては、係長

イ　分庁舎にあっては、課長代理が配置されている課は課長代理、その他の課・係は係長

ウ　交番及び駐在所にあっては、所長

(2) 副取扱責任者は、取扱責任者の指示を受け、その事務を処理するものとする。

7　システム管理担当者

(1) システム管理担当者の指名

システムセキュリティ維持管理者は、その管理する電子計算機ごとにシステム管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。

(2) 所掌事務

システム管理担当者は、担当する電子計算機その他の警察情報システムの情報セキュリティに係るシステム管理に関する事務を行う。

(3) 重複指名

システム管理担当者は、同一の者が複数の電子計算機に関して重複して指名されることを妨げない。

8　ネットワーク管理担当者

(1) ネットワーク管理担当者の指名

システムセキュリティ維持管理者は、その管理するネットワーク機器ごとにネットワーク管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。ただし、ネットワーク機器の維持管理に係る事務が軽微であると認められる場合は、システムセキュリティ維持管理者は、ネットワーク管理担当者を指名せず、当該事務をシステム管理担当者に行わせることができる。

(2) 所掌事務

ネットワーク管理担当者は、担当するネットワーク機器その他の警察情報システムに係るデータ伝送に関する監視及び制御その他の情報セキュリティに係るネットワーク管理に関する事務を行う。

(3) 重複指名

ネットワーク管理担当者は、同一の者が複数のネットワーク機器に関して重複して指名されることを妨げない。

第３　情報の分類及び取扱い

1　情報の分類

要綱第５の２の情報の分類は、別表１のとおり実施する。

2　分類が異なる情報の取扱い

機密性、完全性又は可用性のいずれかの情報の分類が異なる情報を一の警察情報システムで取り扱うことについては、次のいずれかに該当するときに限り認めるものとする。

(1) 当該警察情報システムにおいて取り扱う情報のうち、最も上位の分類に応じた情報の管理が可能であるとき。

(2) 警察庁が設置したものについては最高情報セキュリティ管理者の承認、青森県警察が設置したものについては情報セキュリティ管理者の承認を受けたとき。

3　情報の分類及び通知

(1) 情報セキュリティ管理者は、警察情報システムで取り扱われる情報について、

当該情報に係る業務を主管する所属長及び当該情報を取り扱う警察情報システムシステムセキュリティ責任者と協議の上、分類するものとする。

(2) 情報セキュリティ管理者は、(1)の規定に基づく情報の分類を関係所属に通知するものとする。

(3) 情報セキュリティ管理者は、情報の分類を変更する必要がある場合には、当該情報に係る業務を主管する所属長と協議し、必要な見直しを行わなければならない。

(4) 情報セキュリティ管理者は、(1)の規定に基づく情報の分類を警察庁情報セキュリティ管理者に報告しなければならない。

4　情報の取扱い

(1) 一般的な措置

ア　情報の作成、入手及び利用

(ｱ) 職員は、情報を不正に作成し、利用し、又は処分若しくはき損してはならない。

(ｲ) 職員は、情報を不当な目的で入手し、複製し、又は他の者に提供してはならない。

(ｳ) 職員は、情報を警察の庁舎外に不正に持ち出してはならない。

(ｴ) 職員は、警察庁情報セキュリティ管理者が認めた場合を除き、情報の分類を他の者が認識できる方法を用いて明示しなければならない。

イ　情報の管理

職員は、情報の分類に応じて、警察情報システム、外部記録媒体、ドキュメント及び入出力資料の紛失、盗難の防止に対して十分に配意し、適切に管理しなければならない。

ウ　情報の提供

(ｱ) 職員は、情報を公表する場合には、当該情報が別表１において機密性低に分類される情報であることを確認しなければならない。

(ｲ) 職員は、電磁的記録を公表又は提供する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置を執らなければならない。

エ　情報の消去

(ｱ) システムセキュリティ責任者は、電子計算機及びネットワーク機器を廃棄し、又は利用を終了する場合には、システム管理担当者又はネットワーク管理担当者に、データ消去ソフトウエア又はデータ消去装置の利用、物理的又は磁気的な破壊等の方法を用いて、すべての情報を復元できないように措置させなければならない。また、システムセキュリティ責任者又はシステムセキュリティ維持管理者はこれを確認しなければならない。

(ｲ) 職員は、電子計算機、ネットワーク機器又は外部記録媒体を他の者へ提

供する場合には、これらに保存された情報を復元できない状態にする必要性の有無を検討し、必要があると認めた情報について、データ消去ソフトウエア、データ消去装置等を用いて、当該情報を復元できないように措置し、システムセキュリティ維持管理者又は運用管理者はこれを確認しなければならない。

(ｳ) 職員は、情報を廃棄する場合には、裁断、データの消去その他の方法により情報を復元できないように措置しなければならない。

(2) 情報の分類に応じた管理措置

情報の分類に応じた措置は、別表２のとおり実施する。

第４　警察情報システムの構成要素についての対策

１　設置環境、維持管理等

(1) 機密性高及び中情報

別表１において機密性高に分類される情報若しくは機密性中に分類される情報に係るデータベース装置若しくはネットワーク機器（施錠された筐体に収容されているものであって電気通信回線から切り離された場合に直ちにそのことが検知できる仕組みを有するもの及び電子計算機（データベース装置を除く。(2)において同じ。）に近接して設置する必要のあるネットワーク機器を除く。）を設置し、又はそれらの装置若しくは機器に係るシステムドキュメントを保管する室（以下「警察情報システム機械室等」という。）は、人及び物の出入りを確実に管理することができ、外部からの侵入及び内部の視認が容易にできない構造の区域としなければならない。

また、警察情報システム機械室等には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置を執らなければならない。

(2) 機密性低、完全性低及び可用性低情報以外の情報

別表１において機密性低、完全性低及び可用性低に分類される情報以外の情報（以下「要保護情報」という。）を取り扱う電子計算機を設置し、それらの機器に係るシステムドキュメントを保管し、又は要保護情報に係る入出力資料及び外部記録媒体を取り扱う場所は、人及び物の出入りを管理することができるように区画された区域とし、電子計算機の画面、システムドキュメント及び入出力資料をその区域の外から視認することができない構造としなければならない。

また、その区域には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置を執らなければならない。

(3) 立入り許可等

情報セキュリティ管理者は、警察情報　システム機械室等に立ち入ることができる者の範囲をあらかじめ定め、システムセキュリティ維持管理者又は運用管理者は、そのうち、必要な者に許可を与えなければならない。また、職員以

外の者が警察情報システム機械室等に立ち入るときは、職員を立ち会わせなければならない。

(4) 警察情報システム機械室等からの持ち出しの記録

警察情報システム機械室等に設置されている警察情報システムを構成する機器、外部記録媒体及びシステムドキュメントを警察情報システム機械室等の外に持ち出そうとする者は、システム管理担当者又はネットワーク管理担当者の立会いの下でこれを行い、その状況を記録しなければならない。

(5) ドキュメント等の整備

システムセキュリティ維持管理者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要なドキュメント及び記録簿を整備し、その内容を常に最新のものとしておかなければならない。

また、システム管理担当者及びネットワーク管理担当者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要な作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

(6) 台帳の整備

情報セキュリティ管理者は、警察情報システムについて一元的に把握し管理するため、必要な事項を記載した台帳を整備しなければならない。

2　機器等の管理

(1) 共通対策

ア　職員は、警察情報システムを構成する機器、外部記録媒体及びドキュメントを適正に管理しなければならない。

イ　職員は、警察情報システムを構成する機器、外部記録媒体及びドキュメントを他の者に不正に交付し又は利用させてはならない。

ウ　職員は、警察情報システムを構成する機器及び外部記録媒体として、個人所有の機器及び外部記録媒体を公務に利用してはならない。

エ　職員は、あらかじめ定められた目的以外の目的で不正に警察情報システムを利用してはならない。

また、警察庁情報セキュリティ管理者又は情報セキュリティ管理者が認めた場合を除き、警察情報システムを構成する機器に電子計算機等を接続又は増設し、若しくは警察情報システムを構成する機器を交換してはならない。

オ　職員は、システムセキュリティ責任者が認めた場合を除き、警察情報システムを構成する機器の改造を行い、又はソフトウエアの追加、削除若しくは変更をしてはならない。

カ　職員は、警察庁情報セキュリティ管理者又は情報セキュリティ管理者が認めた場合を除き、警察情報システムを構成する機器及び外部記録媒体を警察

の庁舎外に持ち出してはならない。

キ　システムセキュリティ責任者は、電子計算機（データベース装置を除く。）について、必要な対策を執らなければならない。

ク　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、データベース装置について、許可のない者が容易に操作できないように所要の措置を執らなければならない。

ケ　システムセキュリティ責任者は、電気通信回線を経由してデータベース装置の保守作業を行う場合は、送受信される情報を暗号化する必要性の有無を検討し、必要があると認めた場合は、当該機能を設けなければならない。

　また、システムセキュリティ維持管理者は、当該保守作業を行う場合には、送受信される情報を暗号化する必要性を検討し、必要があると認めたときは、暗号化しなければならない。

コ　システムセキュリティ責任者は、電子計算機にインストールしてもよいソフトウエア及び警察情報システムの維持管理に利用するソフトウエアを定めなければならない。

　また、システムセキュリティ維持管理者は、これに該当しないソフトウエアが稼働していることを認知した場合は、当該ソフトウエアを停止し、利用を定めたソフトウエアであっても、利用しない機能は無効化しなければならない。

サ　システムセキュリティ責任者は、警察情報システムについて、盗難及び設置場所からの不正な持ち出しを防止するための措置を執らなければならない。

シ　システム管理担当者は、データベース装置の時刻設定を正確なものとしなければならない。

ス　運用管理者は、警察情報システムのうち青森県警察ワイドエリアネットワークシステム（アピーネット）及び青森県警察情報管理システム（アップルネット）の端末装置の移設等が必要な場合は、情報セキュリティ管理者に申請しなければならない。

(2)　持ち出し用ＰＣ対策

ア　システムセキュリティ責任者は、持ち出し用ＰＣについて、必要な対策を執らなければならない。

イ　職員は、持ち出し用ＰＣを警察の庁舎外に持ち出す必要がある場合には、持ち出し期間を明らかにし、システムセキュリティ維持管理者又は運用管理者の許可を得なければならない。

　また、庁舎外に持ち出すことを終了した場合には、当該許可者に対して、その旨を報告しなければならない。

　さらに、当該許可者は、持ち出し期間が満了しているにもかかわらず終了の報告がない場合は、その状況を確認し、必要な対応を講じなければならな

い。

ウ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察の庁舎外で持ち出し用ＰＣから無線回線を利用してその他の警察情報システムにアクセスする仕組みを構築してはならない。

3　電子メール及びウェブ

(1) 電子メールの送受信

職員は、業務遂行に係る情報を含む電子メールを送受信する場合には、警察が運営又は外部委託した電子メール機能を利用しなければならない。

また、受信した電子メールについては、適切な方法により表示しなければならない。

(2) 認証機能の設定

システムセキュリティ責任者は、電子メールの送受信時に認証を行う機能を設けなければならない。

(3) 電子メールを保管、中継する電子計算機の管理

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電子メールを保管、送受信又は中継するために設置される電子計算機及びウェブサービスを提供するために設置される電子計算機を不正に使用されることのないように構築し、管理しなければならない。

(4) 利用者情報の管理

職員及びシステムセキュリティ責任者は、電子メール機能の利用及びウェブサービスの提供に当たって、利用者の情報セキュリティが損なわれることのないように必要な措置を執らなければならない。

4　電気通信回線

(1) 利用の検討

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電気通信回線を利用するに当たっては、当該接続による情報セキュリティの維持に係るリスクを検討しなければならない。

(2) 利用回線

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システムを構成する電気通信回線として、警察庁情報セキュリティ管理者が認めた回線を利用しなければならない。

(3) 外部回線との接続禁止

職員は、警察庁情報セキュリティ管理者が認めた場合を除き、警察情報システムを構成する機器を外部回線に接続し、又は外部回線から警察情報システムにアクセスする仕組みを構築してはならない。

(4) 安全性の確保

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、ネッ

トワーク機器について、許可のない者が容易に操作できないように所要の措置を執らなければならない。

(5) 正確性の確保

ネットワーク管理担当者は、ネットワーク機器の時刻設定を正確なものとしなければならない。

(6) 各担当者の協力

ネットワーク管理担当者は、警察情報システムを構成する電気通信回線の監視をシステム管理担当者と協力して行わなければならない。

また、監視により得られた結果は、消去や改ざんが行われないよう適切に管理しなければならない。

第５　情報セキュリティ要件の明確化に基づく対策

１　情報セキュリティについての機能

(1) アクセス制御機能等

ア　システムセキュリティ責任者は、アクセス権者以外の者によるアクセス及びアクセス権者によるアクセス範囲を越えたアクセスを防止するために、整備する警察情報システムごとに認証、アクセス制御及び権限管理を行う機能を設けなければならない。

また、アクセス権者及び各アクセス権者のアクセス範囲を定める場合は、当該警察情報システムで取り扱う情報に係る業務を主管する所属長と協議の上、整備する警察情報システムごとに、必要な手続きを明確化し、業務上の責務と必要性を勘案して、必要最小限の範囲に限らなければならない。

イ　職員は、自己のユーザＩＤ以外のユーザＩＤを用いて、警察情報システムを利用してはならない。

ウ　職員は、自己のユーザＩＤ及びパスワード（以下「ユーザＩＤ等」という。）を他人に知らせてはならない。

また、自己のユーザＩＤ等を他人に知られないように適切に管理しなければならない。ただし、人事異動、長期休暇等に伴う引継ぎのために特に設定したユーザＩＤ等及びあらかじめ複数の者が共用することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。

エ　職員は、ＩＣカード等による認証を用いる場合には、ＩＣカード等を本人が意図せずに使用されることがないように安全措置を執るとともに、紛失しないよう管理し、他人に付与及び貸与してはならない。ただし、あらかじめ複数の者が共用することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。

また、ＩＣカード等を利用する必要がなくなった場合には、これをシステムセキュリティ維持管理者に返納するなどの適切な措置を執らなければなら

ない。

オ　職員は、警察情報システムに設けられた機能を用いて、当該警察情報システムに保存される情報の分類に従って、必要なアクセス制御の設定をしなければならない。

カ　システムセキュリティ維持管理者は、遠隔地から制御又は監視する警察情報システムについて権限のない者に遠隔地から当該機器が制御又は監視を行うことがないよう厳重に管理しなければならない。

キ　システムセキュリティ維持管理者は、システム管理担当者及びネットワーク管理担当者の権限は、個別の者に付与しなければならない。また、これを他の職員に代理させることはできない。

(2)　証跡管理

ア　システムセキュリティ責任者は、警察情報システムについて、証跡管理を行う必要性の有無を検討し、必要があると認めた警察情報システムには、証跡を取得する機能を設けなければならない。

イ　システムセキュリティ維持管理者は、警察情報システムに設けられた機能を利用して、事象ごとに必要な項目を証跡として記録し、管理しなければならない。また、その記録を必要に応じて分析し、適切な措置を執らなければならない。

ウ　システムセキュリティ維持管理者は、システム管理担当者、ネットワーク管理担当者及び職員に対して、証跡の管理、分析等を行う可能性があることをあらかじめ周知しなければならない。

エ　運用管理者は、所属の警察情報システムのアクセス権者及びアクセス範囲を適正に管理しなければならない。

(3)　暗号と電子署名

ア　システムセキュリティ責任者は、警察情報システムにおいて暗号化又は電子署名の付与に用いるアルゴリズムを警察庁情報セキュリティ管理者が定めたものから選定するとともに、暗号化された情報の復号又は電子署名の付与に用いる鍵の管理について定めなければならない。

イ　システムセキュリティ維持管理者は、電子署名の付与を行う必要があると認めた警察情報システムについて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供しなければならない。

ウ　職員は、暗号化された情報の復号又は電子署名の付与に用いる鍵の管理を適正に行わなければならない。

２　特定脅威等への対策

(1)　セキュリティホール対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電子計算機及びネットワーク機器の構築及び運用開始時に、当該機器上で利用

するソフトウエアに関連する公開されたセキュリティホールについて対策を講じなければならない。

イ　システム管理担当者及びネットワーク管理担当者は、管理対象となる電子計算機及びネットワーク機器に関連する公開されたセキュリティホールの情報の入手に努めなければならない。また、その情報を入手した場合には、システムセキュリティ責任者及びシステムセキュリティ維持管理者に報告しなければならない。

ウ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが警察情報システムにもたらすリスクを分析した上で、セキュリティホール対策計画を作成し、これに基づいたセキュリティホール対策を講じるとともに､随時職員に周知しなければならない。

エ　システムセキュリティ維持管理者は、定期的にセキュリティホール対策及びソフトウエア構成の状況を記録し、これを確認、分析するとともに、不適切な状態にある電子計算機及びネットワーク機器を把握した場合には適切に対処しなければならない。

オ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、システムセキュリティ維持管理者及び他のシステムセキュリティ責任者と共有しなければならない。

(2) 不正プログラム対策

ア　職員は、コンピュータ・ウイルス等不正プログラムが電子計算機及び外部記録媒体に存在していないことを確認しなければならない。

　また、不正プログラムが発見された場合には、直ちに拡散の防止のための措置を執らなければならない。

イ　情報セキュリティ管理者は、不正プログラム感染の回避を目的とした職員に対する留意事項を含む日常的実施事項を定めなければならない。

ウ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、不正プログラムから電子計算機（当該電子計算機で動作可能なコンピュータ・ウイルス対策ソフトウエア等が存在しないものを除く。）を保護するための対策を講じなければならない。また、不正プログラム対策の状況を適宜把握し、その見直しを行わなければならない。

(3) IPv6技術を利用する通信への対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システムにIPv6技術を利用する通信（以下「IPv6通信」という。）の機能を導入する場合には、他の警察情報システムの情報セキュリティが損なわれることのないように必要な措置を執らなければならない。

イ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、IPv6通信を想定していない電気通信回線に接続するすべての電子計算機及び

ネットワーク機器について、IPv6通信を停止するための機能を有している場合には、当該機能の設定を適切に行わなければならない。

(4) 踏み台対策

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、外部回線に接続する警察情報システムが、不正アクセス等の中継地点として使用されることを防止するため、(1)及び(2)に掲げるもののほか、必要な措置を執らなければならない。また、不正アクセス等の中継地点として使用された場合の影響が最小となるように警察情報システムを構築しなければならない。

3　警察情報システムのセキュリティ要件

(1) 警察情報システムの計画・設計

ア　システムセキュリティ責任者は、警察情報システムのセキュリティ要件を決定し、その要件を満たすために機器等の購入（購入に準ずる賃貸借契約を含む。）及びプログラム開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに警察情報システムの構成要素についての対策について定めなければならない。

イ　システムセキュリティ責任者は、構築する警察情報システムに重要なセキュリティ要件があると認めた場合には、当該警察情報システムのセキュリティ機能の設計について第三者機関によるＳＴ（Security Target：セキュリティ設計仕様書）評価・ＳＴ確認を受けなければならない。ただし、警察情報システムを改修する場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

ウ　システムセキュリティ責任者は、構築した警察情報システムの運用を開始するに当たって、情報セキュリティの観点から実施する運用開始のための手順及び環境を定めなければならない。

(2) 警察情報システムのセキュリティ要件

ア　警察情報システムの構築、運用及び監視

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行わなければならない。

イ　警察情報システムの移行又は廃棄

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システムの移行又は廃棄を行う場合は、情報の消去及び保存並びに警察情報システムの再利用について必要性を検討し、適切な措置を執らなければならない。

ウ　警察情報システムの見直し

システムセキュリティ責任者は、警察情報システムの情報セキュリティ対

策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を執らなければならない。

4　外部委託

(1)　事業者の選定

外部委託に当たっては、委託によって情報セキュリティが損なわれることのないよう、十分に検討の上、委託先には事業継続性を有すると認められる事業者を選定しなければならない。

(2)　委託時の遵守事項等

職員は、警察情報システムの開発、運用管理、維持管理等を外部委託する場合は、あらかじめ当該委託に係る作業を監督する職員の任務を定めるとともに、当該委託に係る業務の実施の場所及び方法、当該委託に係る業務に従事する者の範囲、委託先によるアクセスを認める範囲その他警察情報システムの情報セキュリティの観点から委託の相手方に遵守させるべき事項を明記した仕様書等を作成しなければならない。

また、契約に当たっては、当該事項を遵守させるための措置を定めるなど情報セキュリティの維持に関し所要の措置を執らなければならない。

(3)　仕様書公開の確認

職員は、警察情報システムに係る仕様書で一般に公開されるものを作成する場合は、当該仕様書が情報セキュリティの観点から支障のないものであることについて、あらかじめ情報セキュリティ管理者の指定する者の確認を受けなければならない。

5　業務継続計画との整合的運用の確保

情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者は、業務継続計画（優先度が高い業務の継続性を確保するために必要な事項を定めたものをいう。以下同じ。）を策定する場合には、業務継続計画と警察情報セキュリティポリシーの整合的な運用が可能となるよう必要な措置を執らなければならない。

第６　事案発生時の措置

1　対処方法等の策定及び周知

情報セキュリティ管理者は、障害・事故等の事案について、その態様、対処方法、連絡体制、報告手順等当該事案を迅速かつ的確に措置するために必要な事項を定め、職員に周知しなければならない。

2　職員等の責務

情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者、運用管理者及び職員は、障害・事故等の事案発生時に、情報セキュリティ管理者が定める事項に基づき、必要な措置を執らなければならない。

3　事案の原因調査と再発防止策

(1) 情報セキュリティ管理者は、障害・事故等の事案が発生した場合には、当該事案の原因を調査し再発防止策を策定しなければならない。また、当該事案の重要性にかんがみ、その調査結果を最高情報セキュリティ管理者に報告する必要がある場合には、警察庁情報セキュリティ管理者を通じて最高情報セキュリティ管理者に報告しなければならない。

(2) 最高情報セキュリティ管理者は、情報セキュリティ管理者から障害・事故等の事案について報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を執らなければならない。

4　警察情報セキュリティポリシー違反時の対応

(1) 最高情報セキュリティ管理者は、３の(1)による報告を受けた事案が、職員が警察情報セキュリティポリシーに違反して警察情報システムを使用したことによる場合には、期間を定め、当該職員に警察情報システムを使用させないことができる。

(2) 最高情報セキュリティ管理者は、３の(1)による報告を受けた事案が、都道府県警察の警察情報システムに係る警察情報セキュリティポリシーの違反である場合には、当該警察情報システムの警察庁との接続を停止することができる。

第７　自己点検及び教養

1　自己点検

(1) 情報セキュリティ管理者は、情報セキュリティの維持の実施状況の自己点検を行うための実施計画を年度ごとに定めるものとする。

(2) 情報セキュリティ管理者は、(1)の実施計画に基づき、職員の警察情報セキュリティポリシーにおける職務に応じた自己点検票及び自己点検の実施手順を定め、職員に対して自己点検の実施を指示しなければならない。

(3) 職員は、情報セキュリティ管理者の指示に従い、自己点検を実施し、その結果自身が改善すべき事項があった場合は改善し、その結果について情報セキュリティ管理者の評価を受けなければならない。

(4) 情報セキュリティ監査においては、自己点検の適正性の確認を行うものとする。

2　教養

情報セキュリティ管理者は、警察情報セキュリティポリシーを正しく理解し、これを確実に実施できるようにするため、職員に対し、職務に応じた教養を行うための体制を整備しなければならない。

第８　その他

1　警察情報セキュリティポリシーに係る情報の管理

職員は、警察情報セキュリティポリシーのうち、公知となることによって警察情報システムに係る犯罪、不正行為等による情報の漏えいその他の情報セキュリティの侵害事案の発生が懸念され、又は公知となることによって既存の警察情報

システムに新たな情報セキュリティに係る対策を講じる必要が生じるものについては、部外に公開してはならない。

2　警察情報セキュリティポリシーの見直し

警察情報セキュリティポリシーの規定については、見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行わなければならない。

3　その他

この対策基準に定めるもののほか、警察情報システムに係る情報セキュリティの維持に関し必要な細目的事項は、別に定める。

別表１　情報の分類

１　機密性の分類

分類	情報の種類
機密性高	警察情報システムにおいて取り扱われている情報のうち、秘密文書の内容に相当する情報その他の機密性が損なわれることによる影響が大きいもの
機密性中	警察情報システムにおいて取り扱われている情報のうち、直ちに一般に公開することを前提としていないもの
機密性低	警察情報システムにおいて取り扱われている情報のうち、機密性高又は機密性中に分類される情報以外の情報

２　完全性の分類

分類	情報の種類
完全性高	警察情報システムにおいて取り扱われている情報（書面を除く。）のうち、改ざん又は滅失した場合に業務の的確な遂行に支障を及ぼすおそれがあるもの
完全性低	警察情報システムにおいて取り扱われている情報（書面を除く。）のうち、完全性高に分類される情報以外の情報

３　可用性の分類

分類	情報の種類
可用性高	警察情報システムにおいて取り扱われている情報（書面を除く。）のうち、その情報が使用できないときに業務の安定的な遂行に支障を及ぼすおそれがあるもの
可用性低	警察情報システムにおいて管理されている情報のうち、可用性高に分類される情報以外の情報

別表２　情報の分類に応じた管理措置

分　類	取　扱　制　限	
	職　　員	情報セキュリティ管理者等
要保護情報（機密性高、機密性中、完全性高、可用性高）	○　情報を放置してはならない。 ○　情報を不正に庁舎外に持ち出してはならない。また、警察情報システム若しくは外部記録媒体を庁舎外へ持ち出す場合又は庁舎外で情報処理を行う場合には、システムセキュリティ維持管理者又は運用管理者の許可を得るとともに、定められた安全管理措置を執らなければならない。 ○　情報の移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを決定し、移送手段を決定し、運用管理者に届け出なければならない。 ○　情報を部外に提供する場合には、提供先において、当該情報が適切に取り扱われるための措置を執らなければならない。	（システムセキュリティ維持管理者） ○　警察情報システム又は外部記録媒体を庁舎外へ持ち出す場合には、当該持ち出し係る記録を取得しなければならない。 （システムセキュリティ責任者） ○　情報セキュリティ管理者が認めた場合を除き、警察情報システムについて、外部からの侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域に設置しなければならない。 ○　持ち出し用ＰＣについて、アクセス制御等庁舎内で利用する警察情報システムと同等の対策が機能するように構成しなければならない。また、盗難を防止するための措置を執らなければならない。 ○　警察情報システムについて、警察情報システムについて、必要に応じて、取り扱う情報が適切なものであることを保証するための機能を設けなければならない。
要機密情報（機密性高、機密性中）	○　情報を必要以上に配付してはならない。 ○　警察庁情報セキュリティ管理者が認めた場合を除き、警察の庁舎外に設置されている機器に情報を保存してはならない。 ○　警察庁情報セキュリティ管理者が認めた場合を除き、外部回線に接続する警察情報システムにおいて、情報を取り扱ってはならない。 ○　情報を移送する場合又は警察情報システム若しくは外部記録媒体に情報を保存する場合には、必要	（運用管理者） ○　アクセス権者及びアクセスの範囲について、必要に応じて見直しを行わなければならない。 （システムセキュリティ責任者） ○　警察情報システムについて、必要に応じて暗号化を行う機能を設けなければならない。 ○　持ち出し用ＰＣについて、電磁的記録媒体に保存される情報の暗号化を行う機能を設けなければならない。

	に応じて当該情報にパスワードを設定し又は暗号化しなければならない。 ○　持ち出し用ＰＣを庁舎外に持ち出す場合には、利用環境に配意し、関係のない者に当該情報を視認されないようにしなければならない。	
機密性高	○　情報を必要以上に複製してはならない。 ○　情報を移送又は外部への提供する場合には、運用管理者の許可を得なければならない。 ○　情報セキュリティ管理者が認めた場合を除き、職員が維持管理を行う警察情報システム以外のものにおいて情報を取り扱ってはならない。	
機密性中	○　運用管理者が届け出を要しないと定めた場合を除き、情報を移送する場合又は外部へ提供には、運用管理者に届け出なければならない。	
要保全情報（完全性高）	○　情報が事実と合致するよう、情報入手時における確認、臨時の点検、補正等の措置を確実に実施しなければならない。 ○　情報を移送する場合又は警察情報システム若しくは外部記録媒体に情報を保存する場合には、必要に応じて電子署名の付与又はバックアップを取得し若しくは複写しなければならない。	（システムセキュリティ責任者） ○　警察情報システムについて、電子署名の付与又は検証を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けなければならない。 ○　警察情報システム、外部記録媒体及びドキュメントについて、必要に応じてバックアップを取得し又は複写した上で、適切に保管しなければならない。
要安定情報（可用性高）	○　情報を移送する場合には、移送中の滅失、紛失等のおそれがあるため、必要に応じて、同一の情報と異なる経路手段で移送するなど適切な措置を執らなければならな	（システムセキュリティ責任者） ○　警察情報システムについて、電子計算機に求められるシステム性能名並びに電気通信回線及びネットワーク機器に求められる通信性能を、将来の見通しを含め

	い。	確保しなければならない。 ○　データベース装置について、必要に応じて冗長構成としなければならない。 ○　警察情報システムの設置に当たって、必要に応じて自然災害等に起因する障害を未然に防止する措置を執らなければならない。また、当該障害が発生した場合の対応手順を定めなければならない。 ○　警察情報システム、外部記録媒体及びドキュメントについて、必要に応じてバックアップを取得し又は複写した上で、適切に保管しなければならない。 ○　警察情報システムについて、電気通信回線に与える負荷を評価するとともに、必要に応じて負荷を継続的に測定し、適切な措置を執らなければならない。 （システムセキュリティ維持管理者） ○　外部回線と接続している警察情報システムについて、電子計算機、電気通信回線及びネットワーク機器に設けられている機能をサービス不能攻撃対策に活用しなければならない。